Deutscher Bundestag **Drucksache 19/929**

19. Wahlperiode 21.02.2018

Kleine Anfrage

der Abgeordneten Andrej Hunko, Christine Buchholz, Anke Domscheit-Berg, Heike Hänsel, Ulla Jelpke, Niema Movassat, Thomas Nord, Dr. Alexander S. Neu, Tobias Pflüger, Martina Renner, Eva-Maria Elisabeth Schreiber, Dr. Kirsten Tackmann, Kathrin Vogler und der Fraktion DIE LINKE.

Beteiligung an Cyberübungen der EU und der NATO in 2018

Unter der estnischen Ratspräsidentschaft hat die Europäische Union im vergangenen Jahr Cyberübungen zur gemeinsamen Krisenbewältigung durchgeführt (Bundestagsdrucksache 18/13503). Den Anfang macht die eintägige Stabsübung „EU CYBRID 2017", in deren Simulation ein EU-Hauptquartier „multiplen Cyberattacken" ausgesetzt war. Wenige Wochen später folgt die Übung „EU PACE 17", bei der „eine erhebliche Anzahl von EU-Mitgliedstaaten" von Cyberangriffen „unterschiedlicher Natur und Intensität" betroffen gewesen sein soll. Die Szenarien in „EU CYBRID 2017" und „EU PACE 17" sollten „die grenzüberschreitende und ressortübergreifende Zusammenarbeit im Krisenmanagement in einem hybriden Umfeld" üben. Während der simulierten Störungen waren die Teilnehmenden unter anderem von einem „erhöhtem und gesteuertem Falschmeldungsaufkommen" betroffen. In einer späteren Phase nahmen die Ministerien und Behörden an der parallel verlaufenden NATO-Übung „CMX 17" teil. Auch die dortigen Übungsszenarien umfassten „Fake News". Zu den Teilnehmenden gehörte das NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), das sich wie die EU-Übungsleitung ebenfalls in Tallinn befindet. Aus Deutschland waren das Verteidigungsministerium und die Bundeswehr beteiligt.

Während der Übungen wurden täglich neue Ereignisse („Injektionen") simuliert. Die britische Bürgerrechtsorganisation Statewatch hatte hierzu ein Planungspapier veröffentlicht (http://gleft.de/26o). Demnach wurden in „EU PACE 17" gleich mehrere Bedrohungen für die Europäische Union angenommen. Ein „quasi-demokratisches Land" stellte sich dabei mit seiner wirtschaftlichen und militärischen Macht gegen die Europäische Union. Aus Sicht der Fragestellerinnen und Fragesteller war hiermit Russland angedeutet, das in der Übung als „Froterre" bezeichnet wurde. Die Regierung des Fantasiestaates verfügte außerdem über „Hacker, Hacktivisten und nationale Medien", die ebenfalls gegen die Europäische Union zu Felde zogen. Wesentliche Akteure waren die Hackergruppen „APT Fabelwolf" und „APT Schimärenwolf", die vermutlich auf die beiden Russland zugeschriebenen Gruppen APT 28 und APT 29 anspielen. Als zweite große Bedrohung wurde in „EU PACE 17" ein „Neugeborener Extremistenstaat" (NEXSTA) simuliert, der ein weltweites Kalifat erschaffen wolle. Durch Überredung, Druck und Terror wollen die Kalifatskrieger ihre Kultur in Europa verbreiten. Zwar nutzt NEXSTA Mittel der digitalen Propaganda, verfügt aber nur über geringe Cyberfähigkeiten. Zum weiteren Gegenspieler der Europäischen Union machte „EU PACE 17" Geflüchtete im Mittelmeer. Ihre Fluchthelfer wurden im angenommenen Szenario vom Militär in einer „Operation AIFOS" bekämpft: Aus

Sicht der Fragestellerinnen und Fragesteller eine deutliche Anspielung auf die real existierende EU-Militärmission EUNAVFORMED SOPHIA. Außerdem simulierten die EU-Cyberkrieger auch die Bekämpfung einer „Antiglobalisierungsgruppe“. Sie wurde in dem Szenario als internationale Bewegung beschrieben, deren besondere Fähigkeit im „Organisieren von Krawallen, die sich als Demonstrationen tarnen“, liegt. Geld für ihre Aktionen erhält die „Antiglobalisierungsgruppe“ vom Fantasiestaat „Froterre“.

Schließlich hat sich die Bundeswehr im vergangenen Jahr auch an der „NATO-Cyber-Abwehr-Übung Locked Shields 2017“ beteiligt (Bundestagsdrucksache 18/13503). Als Szenarien wurden galten „Verunstaltung von Webseiten, Verbreitung von Falschmeldungen, Datendiebstahl von Benutzernamen und Passwörtern, Übernahme der Steuerung von militärischen Drohnen, Ausschalten der Energieversorgung eines Militärflughafens, Kontrolle über die Flugzeugbetankungsanlage“.

Wir fragen die Bundesregierung:

1. Was ist der Bundesregierung über die Planungen für eine Krisenmanagementübung „PACE18“ bekannt?
   a) Wann und wo findet die Übung nach gegenwärtigem Stand statt (sofern die Übung in einzelne Teile aufgegliedert ist, diese bitte benennen)?
   b) Welche Szenarien werden dort geübt
   c) Wer ist mit der Planung und Koordinierung beauftragt?
   d) Wer soll an der Übung teilnehmen bzw. wer wird hierzu (auch als Beobachter) eingeladen?
   e) Welche Vorübungen sollen hierzu abgehalten werden?
   f) Wann und wo finden diese Vorübungen nach gegenwärtigem Stand statt, und wer ist mit der Koordinierung beauftragt?
   g) Mit welchen Kapazitäten wird sich die Bundesregierung nach gegenwärtigem Stand an „PACE 18“ beteiligen?
2. Wann und wo wurde bzw. wird die Krisenmanagementübung „PACE17“ ausgewertet?
3. Welche Schlussfolgerungen („Lessons Learned“) zieht die Bundesregierung aus der Durchführung und Auswertung der Krisenmanagementübung „PACE17“?
4. Was ist der Bundesregierung über die Planungen für eine Krisenmanagementübung „EU CYBRID 2018“ bzw. eine ähnliche, aber anderslautende Veranstaltung bekannt?
   a) Wann und wo findet die Übung nach gegenwärtigem Stand statt (sofern die Übung in einzelne Teile aufgegliedert ist, diese bitte benennen)?
   b) Welche Szenarien werden dort geübt
   c) Wer ist mit der Planung und Koordinierung beauftragt?
   d) Wer soll an der Übung teilnehmen bzw. wer wird hierzu (auch als Beobachter) eingeladen?
   e) Welche Vorübungen sollen hierzu abgehalten werden?
   f) Wann und wo finden diese Vorübungen nach gegenwärtigem Stand statt, und wer ist mit der Koordinierung beauftragt?
   g) Mit welchen Kapazitäten wird sich die Bundesregierung nach gegenwärtigem Stand an „EU CYBRID 2017“ beteiligen?

5. Wann und wo wurde bzw. wird die Krisenmanagementübung „EU CYBRID 2017“ ausgewertet?

6. Welche Schlussfolgerungen („Lessons Learned“) zieht die Bundesregierung aus der Durchführung und Auswertung der Krisenmanagementübung „EU CYBRID 2017“?

7. Was ist der Bundesregierung über die Planungen für eine Krisenmanagementübung „CMX 18“ bzw. eine ähnliche, aber anderslautende Veranstaltung der NATO bekannt?

   a) Wann und wo findet die Übung nach gegenwärtigem Stand statt (sofern die Übung in einzelne Teile aufgegliedert ist, diese bitte benennen)?

   b) Welche Szenarien werden dort geübt

   c) Wer ist mit der Planung und Koordinierung beauftragt?

   d) Wer soll an der Übung teilnehmen bzw. wer wird hierzu (auch als Beobachter) eingeladen?

   e) Welche Vorübungen sollen hierzu abgehalten werden?

   f) Wann und wo finden diese Vorübungen nach gegenwärtigem Stand statt, und wer ist mit der Koordinierung beauftragt?

   g) Mit welchen Kapazitäten wird sich die Bundesregierung nach gegenwärtigem Stand an „CMX 17“ beteiligen?

8. Wann und wo wurde bzw. wird die Krisenmanagementübung „CMX 17“ ausgewertet?

9. Welche Schlussfolgerungen („Lessons Learned“) zieht die Bundesregierung aus der Durchführung und Auswertung der Krisenmanagementübung „CMX 17“?

10. Was ist der Bundesregierung über die Planungen für eine Krisenmanagementübung „Locked Shields 2018“ bzw. eine ähnliche, aber anderslautende Veranstaltung der NATO bekannt?

   a) Wann und wo findet die Übung nach gegenwärtigem Stand statt (sofern die Übung in einzelne Teile aufgegliedert ist, diese bitte benennen)?

   b) Welche Szenarien werden dort geübt

   c) Wer ist mit der Planung und Koordinierung beauftragt?

   d) Wer soll an der Übung teilnehmen bzw. wer wird hierzu (auch als Beobachter) eingeladen?

   e) Welche Vorübungen sollen hierzu abgehalten werden?

   f) Wann und wo finden diese Vorübungen nach gegenwärtigem Stand statt, und wer ist mit der Koordinierung beauftragt?

   g) Mit welchen Kapazitäten wird sich die Bundesregierung nach gegenwärtigem Stand an „Locked Shields 2018“ beteiligen?

11. Wann und wo wurde bzw. wird die Krisenmanagementübung „Locked Shields 2017“ ausgewertet?

12. Welche Schlussfolgerungen („Lessons Learned“) zieht die Bundesregierung aus der Durchführung und Auswertung der „Locked Shields 2017“?

13. Für wie realistisch hält die Bundesregierung die in der „NATO-Cyber-Abwehr-Übung Locked Shields 2017“ angenommenen Szenarien „Verunstaltung von Webseiten“, „Datendiebstahl von Benutzernamen und Passwörtern“, „Übernahme der Steuerung von militärischen Drohnen“, „Ausschalten der Energieversorgung eines Militärflughafens“, „Kontrolle über die Flugzeugbetankungsanlage“?
    a) Bei welchen Gelegenheiten war die Bundesregierung mit entsprechenden Vorfällen bereits konfrontiert?
    b) Bei welchen dieser Vorfälle waren die Systeme der Behörden bereits zuvor von „verschiedene[n] Angriffe[n], wie z. B. Phishing-Mails, Innentäter oder Ausnutzung technischer Schwachstellen“ betroffen?
14. Welche Aufgaben werden das NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), die „EU Hybrid Fusion Cell” sowie das Kommunikationszentrum „EU STRATCOM EAST“ im Rahmen möglicher Übungen „PACE 18“, „EU CYBRID 2018“, „CMX 18“ (oder anderslautender Veranstaltungen der NATO) und „Locked Shields 2018“ übernehmen?
15. An welchen weiteren Cyberübungen wird sich die Bundeswehr in 2018 beteiligen, und welche Szenarien werden dort geübt?
16. An welchen der Cyberübungen, an denen sich die Bundeswehr in 2018 beteiligt, nimmt auch das „Kommando Computer-Netzwerk-Operationen“ (CNO) teil?
17. Inwiefern hält es die Bundesregierung derzeit für notwendig oder entbehrlich, Cyberübungen auch oberhalb der Schwelle eines bewaffneten Angriffs durchzuführen (bitte begründen)?
18. Welche der Cyberübungen, an denen sich die Bundeswehr in 2018 beteiligt, operieren an der Schwelle eines bewaffneten Angriffs?

Berlin, den 20. Februar 2018

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333